UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,013	01/18/2002	David Kammer	035451-0170 (3708.PALM)	2103

26371 7590 07/30/2009

FOLEY & LARDNER LLP
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of Allowability	Application No.	Applicant(s)	
	10/053,013	KAMMER ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the communication filed on 03/27/2009*.

2. ☒ The allowed claim(s) is/are *1-10,12-14,18-25,27,30,31,35-48 and 50-53*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/SHANTO M ABEDIN/
Examiner, Art Unit 2436

DETAILED ACTION

1. This is a subsequent Notice of Allowability reflecting the changes made to the original examiner's amendments dated on 06/12/2009. The examiner's amendments made in this office action were necessary to correct the dependency of the allowed claims 12 and 13.

2. The examiner notes, the applicant's submissions dated 07/02/2009 were not entered since the submitted proposed amendments were informal (as a part of an interview summary), and have already entered through the original examiner's amendments made on 06/12/2009.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 1-10, 12-14, 18-25, 27, 30-31, 35-48 and 50-53 are pending in the application.

5. Claims 1-10, 12-14, 18-25, 27, 30-31, 35-48 and 50-53 are allowed.

RESPONSE TO ARGUMENTS

6. The applicant's arguments regarding 35 USC 103(a) type rejections are fully considered, and found persuasive, therefore, the previous 35 USC 103 (a) type rejections are withdrawn.

EXAMINER'S AMENDMENT

7. An examiner's amendment to the record appears below. Should the changes and/ or additions be unacceptable to the applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with the applicant's representative Mr. Steven C Becker on June 04, 2009 and July 21, 2009.

Claims 1, 12-13, 18, 30 and 38 have been amended as follows:

Claim 1. (Currently Amended) A method of adjusting security for a network user node in wireless communication with a network based upon the location of the node, comprising:

storing a table comprising a plurality of security settings indexed by location in the memory of the network user node;

determining the location of a network user node;

selecting a single level of security from the plurality of security ~~levels~~ settings stored in the table based on the determined location, wherein at least one of the plurality of security levels is a default security ~~level~~ setting selected based at least on a determination that the table does not have a location corresponding to the determined location or based at least on the location of the network user node being unknown; and

modifying a security protection for the network user node based upon the selected level of security, wherein the step of modifying the security protection for the network user node includes modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted,

wherein the determined location and the security protection for the network user node are updated repeatedly.

Claim 12. (Currently Amended) A method of claim [[11]] 1, wherein the security levels are provided by the user of the network user node for a variety of locations.

Claim 13. (Currently Amended) A method of claim [[11]] 1, wherein the security level is based on the type of location determined for the network user node.

Claim 18. (Currently Amended) A computer system for modifying security settings for wireless communications with a network user node based on the location of the node comprising:

an input device having a communicative coupling with a system for determining the location of a network user node;

a storage device for storing a table of security modifications to be performed based on a plurality of locations for the network user node, the security modifications including a plurality of levels, the security modifications being defined by a user of the network user node;

a processor configured to select a data encryption parameter based on the location and the table of security modifications to change whether wireless data transmitted by the computer system to the user node will be encrypted, wherein the processor is configured to select a default security setting if the location is not determined; and

a communication device capable of transmitting a data signal to the network user node based on the selected data encryption parameter;

wherein the location of the network user node and the security protection for the network user node are updated repeatedly.

Claim 30. (Currently Amended) A method of adjusting security for a network user node having a processor, a memory coupled to the processor, a wireless transceiver, and a physical location determining device, wherein the network user node is in communication with a network based upon the physical location of the node, comprising:

storing a table comprising selectable encryption levels indexed by location for each of a plurality of locations in the memory of the network user node;

receiving physical location information using a network user node;

using the network user node to set security protection for wireless data communication to a default encryption level based at least on a determination that the table does not have a location corresponding to the received physical location or based at least on the location of the network user node being unknown; and

using a network user node to modify security protection for wireless data communication to an encryption level selected from the selectable encryption levels based upon the physical location information;

wherein the table is configurable by a user of the network user node; and

wherein the physical location information and the security protection for the network user node are updated repeatedly.

Claim 38. (Currently Amended) A system implemented on a network user node for modifying security settings based on the physical location of the node comprising:

a system for determining the physical location of the network user node coupled to the network user node;

a processor for processing information, storing information on a storage device, and accessing a table of security modifications, the table configured to store security modifications for more than two physical locations; and

a storage device for storing the table of security modifications;

wherein the network user node performs security modifications based on the physical location of the network user node, wherein the security modifications comprise modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted , wherein a default security setting is selected based at least on a determination that the table does not have a location corresponding to the received physical location or based at least on the location of the network user node being unknown; and

wherein the physical location and the performance of security modifications for the network user node are updated repeatedly.

EXAMINER'S REASONS FOR ALLOWANCE

8. The following is an examiner's statement of reasons for allowances:

Independent claim 1 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach a method of adjusting security for a network user node comprising storing a table comprising a plurality of security settings indexed by location in the memory of the network user node; and selecting a single level of security from the plurality of security settings stored in the table based on the determined location, wherein at least one of the plurality of security levels is a default security setting selected based at least on a determination that the table does not have a location corresponding to the determined location or based at least on the location of the network user node being unknown; and modifying a security protection for the network user node based upon the selected level of security, wherein the step of modifying the security protection for the network user node includes modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted; and wherein the determined location and the security protection for the network user node are updated repeatedly.

Independent claim 18 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach a computer system comprising storing a table of security modifications to be performed based on a plurality of locations for the network user node, the security modifications including a plurality of levels, the security modifications being defined by a user of the network user node; selecting a data encryption parameter based on the location and the table of security modifications to change whether wireless data transmitted by the computer system to the user node will be encrypted, wherein the processor is configured to select a default security setting if the location is not determined; and transmitting a data signal to the network user node based on the selected data encryption parameter; and

wherein the location of the network user node and the security protection for the network user node are updated repeatedly.

Independent claims 30 and 38 are patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach a method/ system comprising storing information on a storage device, and accessing a table of security modifications, the table configured to store security modifications for more than two physical locations; and wherein the network user node performs security modifications based on the physical location of the network user node, wherein the security modifications comprise modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted , wherein a default security setting is selected based at least on a determination that the table does not have a location corresponding to the received physical location or based at least on the location of the network user node being unknown; and wherein the physical location and the performance of security modifications for the network user node are updated repeatedly.

In particularly, regarding the independent claims, patentability exists, at least in part, with the recitation of security modification is defined, or performed, or configured by the user node, and security setting table includes plurality of security settings including a default security, and encryption level associated with the plurality of locations ; and selectively updating, or modifying the security protection or level for the user node repeatedly.

Dependent claims are allowed because of their dependency on the allowable independent claims.

CONCLUSION

9. Claims 1-10, 12-14, 18-25, 27, 30-31, 35-48 and 50-53 are patentable.

10. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on Statement of Reasons for Allowance."

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, A.U. 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436